REMARKS

I. In the Specification

Amendments to the specification in Applicant's previous Amendment and Response of February 01, 2008 have been rejected under 35 USC §132(a) because the Examiner believes that the amendments add new matter to the specification.

Applicant respectfully submits that for at least the reasons set forth below, and in view of the background information submitted relating the basics of quantum key distribution, ***no new matter was added to the specification in the previous Amendment and Response***.

Applicant therefore requests that the Examiner reconsider his rejection of the Amendments to the specification in the previous Amendment and Response of February 01, 2008, in light of the discussion below, and that the rejection of the Amendments to the specification be withdrawn and the Amendments entered.

Information regarding "raw" and "sifted" keys

The amendment to the "Background of the Invention" section that clarifies the meaning of the "raw key" and "sifted key" is basic background information that is known to one skilled in the art. This information is described in the book by Bouwmeester et al., "The Physics of Quantum Information," Springer-Verlag 2001 ("Bouwmeester") in Section 2.3, pages 27-33, which is cited in the "Background of the Invention" section.

Applicant has included pages 27-33 of Bouwmeester herewith. Section 2.3 of Bouwmeester is entitled "Quantum Key Distribution with Single Particles" and discusses the basics of quantum key distribution using single particles in the form of polarized photons. The same basics apply identically with respect to raw and sifted key formation to a quantum key distribution system that phase modulates rather than polarization modulates the photons.

The example described in Section 2.3 and summarized in Table 2.1 on page 29 states what every person skilled in the art of quantum key distribution

knows: ***the formation of raw and sifted keys is fundamental to performing quantum key distribution***.

Applicant's disclosure includes raw key formation and sifted key formation in the "Detailed Description of the Invention" section of the specification.

For example, Applicant's paragraph [0020] reads as follows:

> [0020] With continuing reference to FIG. **1**, in the normal operation of a QKD system such as QKD system **10**, qubits are exchanged between Alice and Bob by controller **20** causing laser **50** to emit weak (e.g., ~0.1 photon) optical pulses. Controller **20** then provides basis and key bits via TRNG **30** (or alternatively via two separate TRNG's **30**) to PM1 to randomly encode the weak pulses. At Bob, controller **120** also causes PM2 to randomly select (via TRNG **120**) a basis to measure and detect the modulated qubits at detector **150**.

One skilled in the art understands this description as constituting the basic steps used in quantum key distribution for forming the "raw key," and is entirely consistent with the description of raw key formation set forth in Bouwmeester.

Applicant's paragraph [0033] and [0034] read as follows.

> [0033] At this point, Bob and Alice run standard QKD procedures (e.g., sifting, error correction, privacy amplification). It is preferable that all information sent during the latter procedures is encrypted with a cipher of the cryptographic strength not lower than the stream cipher. Some information has to be authenticated, as required in the BB84 protocol.
>
> [0034] Alternatively, Alice and Bob can run sifting and/or error correction first and decrypt the bits afterwards. This would require some simple modifications of decryption nmcess.

The "sifting" procedure referred to in these paragraphs is understood by one skilled in the art to constitute the formation of a "sifted key," as described in Bouwmeester. In fact, given that these two paragraphs both use the word ***sifting*** in connection with running ***standard QKD procedures***, the position that the description in Applicant's

specification somehow does not support the formation of a ***sifted key*** defies reason.

Applicant respectfully submits that for at least these reasons, and in view of the supporting material provided in Bouwmeester, the Applicant's addition of clarifying language to the "Background of the Invention" section relating to the "raw" and "sifted" keys is both ***inherently*** an ***expressly*** supported by the specification and so does not constitute the addition of "new matter" to the specification.

<u>Amendments to independent claims 1, 8 and 9</u>

The Examiner states that language added to independent claims 1, 8 and 9 of "without first forming unencrypted qubits from the optical pulses" is not supported by the specification and constitutes "new matter" added to the Application.

In fact, this limitation is ***fully and expressly supported*** by Applicant's specification. For example, Applicant's paragraph [0021] and [0023] through [0028] read as follows:

> [0021] However, as discussed above, there are potential security shortcomings in this QKD process. To address these shortcomings, the present invention further involves encrypting (e.g., at the software level) using e/d module **40** at least the key bits from TRNG **30** used to set Alice's phase modulator state for each qubit. This results in "encrypted qubits" being sent to Bob.

[0023] The method of encrypting Alice's key bits is illustrated in FIGS. **2** and **3**. Suppose there are **b1**, **b2**, . . . bi, . . . bn bits from TRNG **30** for basis and **k1**, **k2**, . . . ki, . . . kn bits to form a set of qubits. In an example embodiment, two TRNGs **30** are used to separately generate the basis and key bits, respectively.

[0024] In an example embodiment of the invention, key-bit values k_i are encrypted by e/d module **30** with a stream cipher (e.g., AES in CTR mode). To do this, Bob and Alice must share a pre-agreed password. The stream cipher is needed because some qubits can be lost in quantum channel **200**. The loss of qubits during transmission precludes the use of other types of ciphers.

[0025] Suppose Alice and Bob share a password P. In an example embodiment, password P is created by either using a fraction of their key generated by QKD. In another example embodiment, password P is created using one of the known method, such as secure currier or Diffie-Hellman protocol. In an example embodiment, Alice and Bob agree to refresh the password P at a chosen rate. Having this password, they can generate a pad **p1**, **p2**, . . . pi, . . . pn by means of a stream cipher

[0026] Once the pad is generated, Alice then performs in e/d module **30** the "exclusive OR" (XOR) operation:

[0027] ki XOR pi=ci

[0028] Alice also sets her phase modulator **PM1** to encode ci on a qubit, not ki. This process is illustrated in the flow diagram of FIG. **3**. The result is what is referred to herein as an "encrypted qubit" or an "encoded qubit."

One skilled in the art understands as axiomatic that in quantum key distribution, a qubit is not formed until an optical pulse is modulated. Since the first modulation in Applicant's invention occurs with an encrypted modulation, it is also axiomatic (i.e., ***inherent***) that in Applicant's invention, the encrypted qubit is formed ***without having formed an unencrypted qubit***. There is simply no other way to encrypt qubits in Applicant's invention.

Accordingly, the amended language for claims 1, 8 and 9 is fully supported by the specification in at least the paragraphs cited above and so does not constitute "new matter."

Amendment to independent claim 5

The Examiner also objects to the amendment to claim 5 that adds the limitation "simultaneously so as to simultaneously encoded {*sic*: encode} and encrypt the optical pulses to form encrypted qubits" and asserts that this constitutes "new matter" that must be canceled.

Applicant respectfully disagrees with the Examiner. With reference to the above-cited paragraphs [0021] and [0023]-[0028], one skilled in the art understands from this enabling disclosure that the encoding of the optical pulse and the encrypting of the optical pulse occur simultaneously through the use of the encrypted key bits. There is no other way to do so in Applicant's invention.

Accordingly, the amended language for claim 5 is fully supported by the specification in at least the above-cited paragraphs and so does not constitute "new matter."

In view of the above reasons, Applicant respectfully requests the withdrawal of the objection to the above-cited amendments to the specification and claims.

In the Claims

Claims 1-13 are pending in the application stand rejected.

Claim 5 has been amended to correct a typographical error.

Claim 10 as been amended to correct the dependency of this claim from itself to claim 8 as kindly pointed out by the Examiner.

I. Claim rejection under 35 USC § 112

Claims 1-4 and 8-13 stand rejected under 35 USC §112, first paragraph, as failing to comply with the written description requirement and for not being enabled.

For at least the reasons discussed above in connection with the objections under 35 USC § 132(a) to the amendments to the specification and claims made in the previous Amendment and Response for being "new matter," Applicant respectfully submits that the amendments to claims 1, 5, 8 and 9 are fully supported by the written description and enablement provided in at least paragraphs [0020] through [0028] of Applicant's specification.

Applicant therefore respectfully requests withdrawal of the rejections under 35 USC §112, first paragraph, of the above-cited claims for failure to satisfy the written description and enablement requirements.

II. Rejections under 35 USC §103

Claims 1 and 9 were rejected over U.S. Patent No. 5,757,912 to Blow ("Blow") in view of U.S. Patent Application Publication No. 2004/0032954 to Bonfrate et al. ("Bonfrate").

An obvious rejection under 35 USC §103(a) requires that the combination of cited references yield all of the claim limitations. Also, the claim must be ***read as a whole*** to avoid the impermissible assembling bits and pieces of prior art to reconstruct Applicant's claimed invention using hindsight.

Claims 1-4

The Examiner correctly points out that Blow does not teach encrypting the key bits and using the encrypted key bits to form encrypted qubits. The Examiner then asserts that "Bonfrate discloses encoding key information and having single optical photons (qubits) [that] carry said encoded key information" (citing Bonfrate paragraph [0007]). This statement stands for the usual prior art proposition that photons are encoded via phase modulation in order to form encoded (but unencrypted) qubits that form an encrypted key. This ***encoding*** is ***not the same*** as using ***encrypted key bits*** to form ***encrypted*** qubits.

A closer reading of Bonfrate reveals that Bonfrate has nothing to do with forming encrypted qubits in the manner claimed by Applicant. Bonfrate discloses a quantum cryptography apparatus that "overcomes problems associated with polarisation evolution in quantum cryptography systems that incorporate a non-polarisation preserving optical channel (e.g., standard optical fiber)." See Abstract. Bonfrate does this by avoiding the use of an active random number generator and phase modulator at the receiver by using a polarization beam splitter (**14**) that serves as a random router. Paragraph [0029]; FIG. 1.

Simply stated, the ***encoding*** performed by Bonfrate is the usual polarization encoding used to form ***unencrypted qubits***. It has nothing to do with forming ***encrypted qubits*** per Applicant's claimed invention. ***There is absolutely no teaching or suggestion in Bonfrate of forming encrypted qubits using encrypted key bits***.

Therefore, the combination of Blow and Bonfrate cannot not yield all of the limitations in Applicant's claim 1. Consequently, a *prima facie* case for obviousness cannot be established using these references.

The obviousness rejection of Applicant's claim 1 is therefore traversed and withdrawal of the rejection is earnestly requested. For the same reasons, the obviousness rejection as applied to dependent claims 2-4 is also traversed and withdrawal of the obviousness rejection of these claims is earnestly requested.

Claims 5-7

Claim 5 is rejected for the same reasons as claim 1, and further in view of the article "Applied Cryptography" by Schneier ("Schneier"). Accordingly, the rejection of claim 5 and its dependent claims 6 and 7 is traversed for the same reasons set forth above in connection with the obviousness rejection of claims 1-4.

Claim 8-13

Claims 8-13 are rejected under 35 USC §103(a) as being unpatentable over U.S. Patent No. 5,675,648 to Townsend ("Townsend") in view of U.S. Patent Application Publication No. 2006/0120529 to Gisen et al. ("Gisen"), and further in view of Schneier and Bonfrate.

Applicant reiterates here that a closer reading of Bonfrate reveals that ***Bonfrate has nothing to do with forming encrypted qubits in the manner claimed by Applicant.*** Bonfrate discloses a quantum cryptography apparatus that "overcomes problems associated with polarisation evolution in quantum cryptography systems that incorporate a non-polarisation preserving optical channel (e.g., standard optical fiber)." See Abstract. Bonfrate does this by avoiding the use of an active random number generator and phase modulator at the receiver by using a polarization beam splitter (**14**) that serves as a random router. Paragraph [0029]; FIG. 1.

The ***encoding*** performed by Bonfrate is the usual polarization encoding used to form ***unencrypted qubits***. It has nothing to do with forming ***encrypted qubits*** per Applicant's claimed invention.

The cited references and the arguments set forth by the Examiner indicate that the Examiner is not reading each claim ***as a whole*** to appreciate and understand the invention ***in its entirety***. The Examiner seems to have fallen into the trap of using the claims as a guide to find references covering different features of the invention

without regard to what the invention covers ***as a whole***. This is impermissible hindsight reconstruction of the claims using the prior art. See, e.g., *In re Fritch*, 972 F.2d 1260, 23 USPQ 2d 1780, 1784 (Fed. Cir. 1992).

All of the cited patent references are directed to the conventional practice of quantum key distribution (QKD) that involved the random modulation of optical pulses to form unencrypted qubits. The Schneier reference is directed to classical encryption, and Applicant's invention admits to using classical encryption since it is invention is entitled "QKD with classical bit encryption." However, it is the ***combination of claim elements taken as a whole*** that combine classical encryption with quantum cryptography in ***a unique and non-obvious way*** to provide enhanced security over existing quantum encryption systems.

There is absolutely no teaching, suggestion or motivation in any of the cited references to form encrypted qubits using encrypted key bits in the manner claimed by the Applicant. Moreover, ***the combination of the cited references cannot yield all of the limitations in Applicant's claims 8-13.*** Consequently, a *prima facie* case for obviousness cannot be established using the cited references.

Accordingly, the obviousness rejection of Applicant's claims 8-13 is traversed and withdrawal of the rejection is earnestly requested.

CONCLUSION

Applicant respectfully submits that claims 1-13 as presently presented are in condition for allowance.

Applicant believes that a **three-month** extension of time extension pursuant to 37 C.F.R. § 1.136(a) in the amount of **$525** is necessary to make this Reply timely, and hereby authorizes the Office to charge any necessary fee or surcharge with respect to said time extension to Deposit Account **502992**

The Examiner is encouraged to contact the Assignee's authorized representative at 941-378-2744 to discuss any questions that may arise in connection with this Amendment.

Respectfully Submitted,

By: ______________________ Date: September 24, 2008

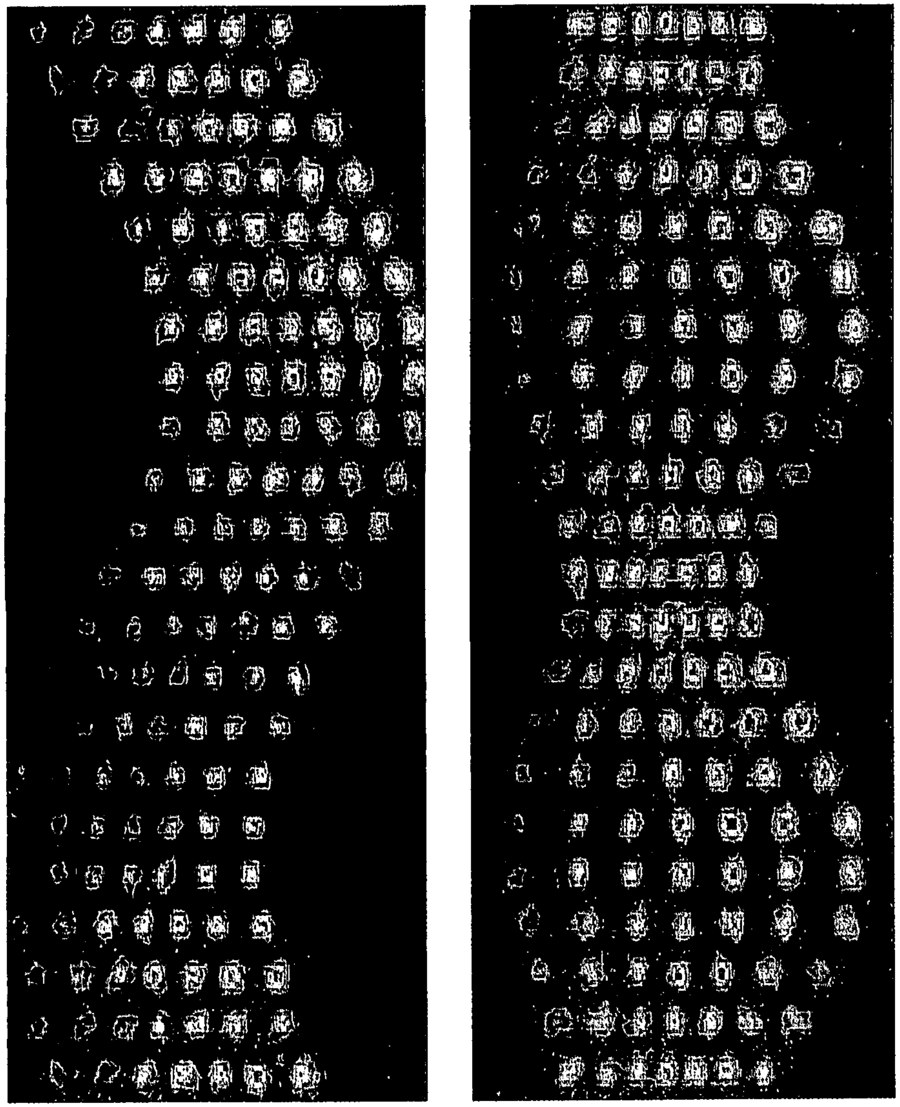
Joseph E. Gortych

Reg. No. 41,791

Customer No. 53590

Opticus IP Law PLLC
7791 Alister Mackenzie Dr
Sarasota, FL 34240 USA

Phone: 941-378-2744
Fax: 321-256-5100
E-mail: jg@opticus-ip.com



Experimental demonstration of the breathing mode (left) and the centre-of-mass motion (right) of a string of 7 ions which form an array of 7 qubits. The figures are compilations of a sequence of snapshots taken of the string of ions (see Chapter 5). Figures by J. Eschner, F. Schmidt-Kaler, R. Blatt, Institut für Experimentalphysik, Universität Innsbruck.

Dirk Bouwmeester
Artur Ekert
Anton Zeilinger (Eds.)

The Physics of Quantum Information

Quantum Cryptography
Quantum Teleportation
Quantum Computation

With 125 Figures

Springer

may contain no photon at all, while others contain 1, 2 or even more photons. Pulses with more than one photon per pulse should be avoided, since they may leak information to an eavesdropper. In order to make the probability of more than one photon per pulse low enough, one needs to use very weak pulses, which in turns reduces the signal to noise ratio. The value generally adopted is 0.1 photon per pulse on average (this really means that only one pulse out of 10 contains a photon), which gives a probability of more than one photon of 5×10^{-3}. This still means that 5 % of the usable pulses (with at least one photon), contain two or more photons, and could leak information to an eavesdropper. Development of a good single photon source seems technologically possible, but has not been achieved yet.

The second, more serious problem for practical applications of QC is that a quantum channel cannot be amplified without losing its quantum properties. Therefore, due to losses in the transmission, QC can operate only over limited distances. For all existing systems, which are based on infrared photons in silica fibres, the minimum loss rate is about 0.2 dB/km. So it seems that QC systems with a range of more than 100 km (with losses of 20 dB, or a transmission rate of 0.01) are not possible for the foreseeable future. Therefore, a transatlantic cable with QC secrecy remains a complete utopia for the time being.

The third problem is that QC is well adapted to point-to-point exchanges, but not so well to other types of networks. Recent proposals suggested some improvements in this direction [41], but these are still limited to one-to-a-few users. QC access for home-to-home transactions is still impractical. However, a kind of Local Area Network, with a central broadcasting station (e.g. the main branch of a bank) and a number of receivers (e.g. the local branches of the bank), is certainly conceivable.

2.3 Quantum Key Distribution with Single Particles

2.3.1 Polarised Photons

Quantum key distribution with polarised photons, as originally proposed by C.H. Bennett and G.Brassard [38, 42], employed pulses of green light in free space, over a distance of 40 cm, and we shall discuss it in some detail. This experiment was obviously not useful for actual key transmission, but represented the first experimental steps of QC. The first implementation of this particular protocol with optical fibres (over a distance of about 1 km) was done at the university of Geneva [43]. Nowadays, distances have reached the tens of kilometers range. In this section, we shall present the principles of QC with polarised photons, leaving the experimental implementations to Sect. 2.6

Let us consider pulses of polarised light, each pulse containing a single photon. We shall begin with polarisation either horizontal or vertical, denoted

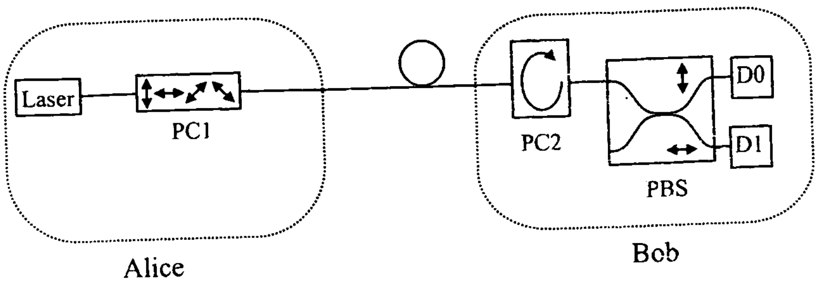


Fig. 2.4. Polarisation scheme: The sender, Alice, sends very weak pulses of polarised light to Bob. The polarisation is controlled by a Pockels cell (PC1), which enables Alice to choose between the four possible polarisations: $|\updownarrow\rangle$, $|\leftrightarrow\rangle$, $|\nearrow\rangle$, $|\nwarrow\rangle$. On Bob's side, a second Pockels cell (PC2) controls the rotation of the setup: 0° corresponds to a measurement in basis $\oplus$, while 45° corresponds to a measurement in basis $\otimes$. The polarisation beamsplitter (PBS) separates the beam into two orthogonal components, which are detected by either D0 or D1 (the setup chosen corresponds to a measurement in $\oplus$).

in the quantum mechanical Dirac notation by $|\leftrightarrow\rangle$ and $|\updownarrow\rangle$ respectively. To transmit information we need a coding system, say $|\updownarrow\rangle$ codes for 0, while $|\leftrightarrow\rangle$ codes for 1. Using this system, the sender, known as Alice, can send any message to the receiver, known as Bob. For example, if Alice sends a series of pulses: $|\leftrightarrow\rangle$, $|\updownarrow\rangle$, $|\leftrightarrow\rangle$, $|\leftrightarrow\rangle$, $|\updownarrow\rangle$; the corresponding binary number is 10110. When she sends either $|\leftrightarrow\rangle$ or $|\updownarrow\rangle$ only, we shall say that Alice sends her photons in the $\oplus$ basis. As the required key needs to be random, Alice will send 0 or 1 with equal probability. In order to detect the message, Bob uses a Polarisation Beamsplitter (PBS) transmitting the vertical polarisation while deflecting the horizontal one. This is followed by single-photon detectors in each arm of the set-up, as shown in Fig. 2.4. Detection in detector D0 (D1) means that Alice sent a 0 (1). In this case, we shall say that Bob detects in the $\oplus$ basis as well. As detectors are not perfect, and also due to possible losses in the transmission, both detectors will often fail to register any photon. In this case, Bob shall tell Alice that he failed to register anything, and the corresponding bit shall be discarded. Therefore, only a fraction of the original bits will be actually used, but the remaining ones should be shared by Alice and Bob. This system is thus useless for sending a given message, but it will be useful to send a cryptographic key, where the only requirements are randomness and confidentiality.

Up to this point, our setup is totally insecure. The eavesdropper, known as Eve, could also measure the pulses with a setup similar to Bob's, and re-send similar pulses to Bob. Eve would then know all the bits shared by Alice and Bob. To obtain confidentiality, Alice adds another random choice: she shall now use either the previous horizontal-vertical polarisations (the $\oplus$ basis); or one of the two linear diagonal polarisations, with $|\nearrow\rangle$ denoting a 0 and $|\nwarrow\rangle$ denoting a 1. Here again, Alice shall send a 0 or 1 with equal probability. This corresponds to the $\otimes$ basis. By rotating his setup by 45°,

Table 2.1. Example of a polarisation protocol. Alice chooses at random a basis ($\oplus$ or $\otimes$) and a bit value (0 or 1), and sends the corresponding polarisation state to Bob. Bob chooses also at random the reception basis, and obtains a given bit. The ensemble of these bits is the raw key. Alice and Bob then tell each other the basis used over the public channel, and keep only the bits corresponding to the same basis. This is the sifted key. They choose at random some of the remaining bits to test for Eve, then discard them. In this case, there are no errors, which indicates that the transmission is secure. The remaining bits form the shared key.

A basis	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\oplus$
A bit value	0	1	0	1	1	0	1	0	0	0	0
A sends	$\vert\nearrow\!\!\!\!\!\swarrow\rangle$	$\vert\leftrightarrow\rangle$	$\vert\updownarrow\rangle$	$\vert\nwarrow\!\!\!\!\!\searrow\rangle$	$\vert\leftrightarrow\rangle$	$\vert\nearrow\!\!\!\!\!\swarrow\rangle$	$\vert\nwarrow\!\!\!\!\!\searrow\rangle$	$\vert\updownarrow\rangle$	$\vert\nearrow\!\!\!\!\!\swarrow\rangle$	$\vert\nearrow\!\!\!\!\!\swarrow\rangle$	$\vert\updownarrow\rangle$
B basis	$\otimes$	$\oplus$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\oplus$
B bit	0	1	0	0	1	0	1	1	0	1	0
Same basis?	y	y	n	n	y	y	y	n	n	n	y
A keeps	0	1			1	0	1				0
B keeps	0	1			1	0	1				0
Test Eve?	y	n			y	n	n				n
Key		1				0	1				0

Bob can also choose to measure in the $\otimes$ basis. Safety is obtained thanks to a fundamental property of quantum mechanics: indeterminism. A single photon pulse prepared in the $\otimes$ basis and measured in the $\oplus$ basis has probability $\frac{1}{2}$ of going towards either detector, D0 or D1. And this choice is purely random: there is nothing in the photon to reveal which way it will go. So if Alice prepares a photon in, say state $|\nearrow\!\!\!\!\!\swarrow\rangle$, and Bob (or anybody else) attempts to measure it in the $\oplus$ basis, he may get a count in either detector, D0 or D1, with equal probability. Let us emphasise that this does not mean at all that half of the photons in a beam of $|\nearrow\!\!\!\!\!\swarrow\rangle$ are polarised vertically and half horizontally. This would be inconsistent with the fact that, when Bob uses the $\otimes$ basis, he always gets a 0. In fact, the systems behaves as if, when it is measured, it chooses randomly which way to go.

Obviously, the above applies equally well to Eve. As Alice uses either basis at random, there is no way for Eve to decide which measurement basis to use. Whenever she uses the wrong basis, she gets a random result, which is not correlated to Alice's choice. Another important point is that Eve cannot know that she got a wrong result: a count in D0 may mean that the photon was prepared in the $|\updownarrow\rangle$ state, but it may also mean that it was in the $|\nearrow\!\!\!\!\!\swarrow\rangle$ or in the $|\nwarrow\!\!\!\!\!\searrow\rangle$ state, and simply "choose" to go towards D0. This is why we do need single-photon pulses: a pulse with more than one photon sent in the wrong basis may give a count in both D0 and D1, thus telling Eve that she used the wrong basis. She could then simply discard the transmission, thus avoiding creating any error. However, when she receives only one photon, Eve has no other choice but to send it on to Bob, in the state that she measured. This will unavoidably create errors in the string received by Bob. The above eavesdropping strategy, known as the intercept-resend strategy is only one of the possibilities available to Eve.

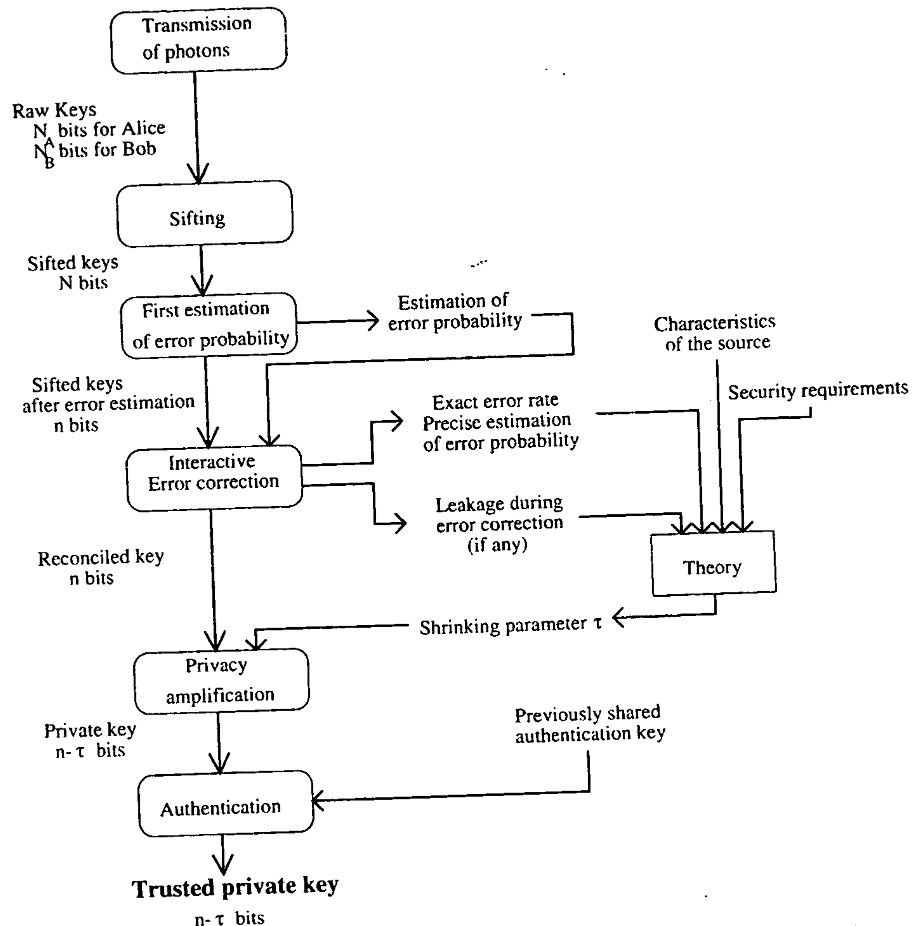


Fig. 2.5. Diagram of single-photon based quantum key distribution protocol

We now have the basic blocks for the polarisation cryptograpy protocol, an example of which is given in Table 2.1. The whole protocol is illustrated in Fig. 2.5 and is summarised as follows:

1. Alice chooses at random both the basis and the polarisation of her single-photon pulses, and sends them to Bob.
2. For each pulse, Bob chooses also at random which basis he will use, and measures the pulse. He either registers the count in D0 or D1, or fails to register anything, due to losses in the detection or in the transmission. The ensemble of all the received bits is the raw key.
3. Bob uses the public channel to tell Alice which photons were registered, and which basis was used. Of course, Bob does not tell the result of the measurement (count in D0 or D1). Alice answers back by telling

which basis she used. Whenever Alice and Bob used the same basis, either ⊕ or ⊗, they should get perfectly correlated bits. However, due to imperfections in the setup, and to a potential eavesdropper, there will be some errors. The ensemble of these bits is the sifted key.

4. To transform their partly corrupted and maybe not entirely secret strings into a usable shared and secret key, Alice and Bob now need some processing. The processing stage is in fact common to all implementations of QC with single particles. The main steps are: to estimate the error rate of the transmission; to infer the maximum information that may have leaked to an eavesdropper; and then to correct all the errors, while reducing the information potentially available to Eve to any level required. The remaining string of bits is the secret key.

Polarisation schemes are very appealing in free space, where polarisation is conserved, but are more complicated to implement in optical fibres, due to depolarisation and randomly fluctuating birefringence. Depolarisation is not a major problem: its effects can be suppressed by means of a sufficiently coherent source. The timescale of the fluctuations of the birefringence in stable conditions is quite slow (1 hour). However, during an experiment on an installed cable, we have also observed much shorter timescales, which rendered transmission impossible. An electronic compensation system, enabling continuous tracking and correction of the polarisation is certainly possible, but requires an alignment procedure between Alice and Bob. This may make the scheme a bit too cumbersome for potential users.

2.3.2 Phase Encoded Systems

Instead of relying on polarisation, which is not easy to control in optical fibres, one can base a QC system on phase encoding. Originally the phase encoding, with optical fibres and the Mach–Zehnder interferometers, was introduced in the context of the entanglement-based quantum cryptography [44], but it can also be used with the single-particle schemes [45]. The theoretical setup is shown in Fig. 2.6. This is an extended Mach–Zehnder interferometer, with Alice on the left, and Bob on the right, with two connecting fibres. Both Alice and Bob have a phase modulator (PM) on their side to enable the coding and decoding. Let us assume for the moment that Bob does not use his PM, and that the interferometer is aligned to have a constructive interference in D0, and a destructive one on D1. If Alice uses her PM to get either 0 or π phase shift (corresponding to bit value 0 and 1), Bob will either get a count in D0 or in D1. This is the equivalent of the previous scheme with two polarisations only. To obtain confidentiality, we add the random choice of basis. Here, this means that Alice shall choose between four phase shifts: 0, π (corresponding to the ⊕ basis), and $\frac{\pi}{2}$, $\frac{3\pi}{2}$ (corresponding to the ⊗ basis). On his side, Bob will also choose between 0 phase shift, i.e. measuring in the ⊕ basis, and

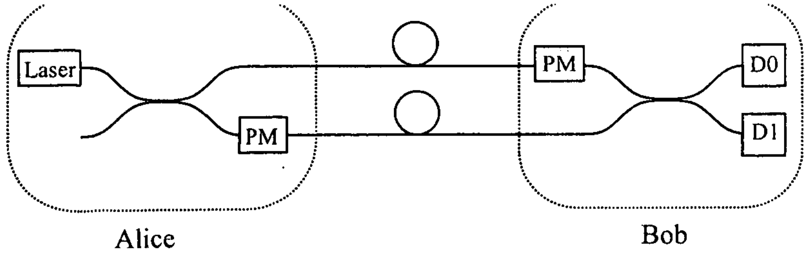


Fig. 2.6. Phase setup with an extended Mach–Zehnder interferometer. The relative choice of phase in the two phase modulators (PM) gives the interference pattern. Alice chooses between four possibilities: 0 or π corresponding to basis $\oplus$; $\frac{\pi}{2}$ or $\frac{3\pi}{2}$ corresponding to basis $\otimes$. Bob chooses between 0 (corresponding to a measurement in basis $\oplus$) and $\frac{\pi}{2}$ (corresponding to $\otimes$). When Alice and Bob use the same basis, a count in D0 means 0, and a count in D1 means 1. When the two bases are different, there are no correlations between the bit sent by Alice and the one received by Bob.

$\frac{\pi}{2}$ phase shift, i.e. measuring in the $\otimes$ basis. This is the equivalent to the previous polarisation scheme.

Unfortunately, keeping the phase difference in such an extended interferometer (each arm should be about 20 km long) is very difficult. Therefore a better practical setup is to collapse the interferometer, as shown in Fig. 2.7. One pulse entering Alice's side of the MZ is split into two. The two pulses propagating one after the other along the single transmission fibre are denoted by S (for short path) and L (for long path). After travelling through Bob's side of the MZ, these create three output pulses. Two of them, noted SS (for short-short) and LL (for long-long) are not relevant, as they show no interference effect. The central one however corresponds to two possible paths: SL or LS, which are indistinguishable and therefore interfere. The choice of the phase shifts by Alice and Bob gives the encoding-decoding, as in the previous paragraph. This setup is much more stable than the previous one, since

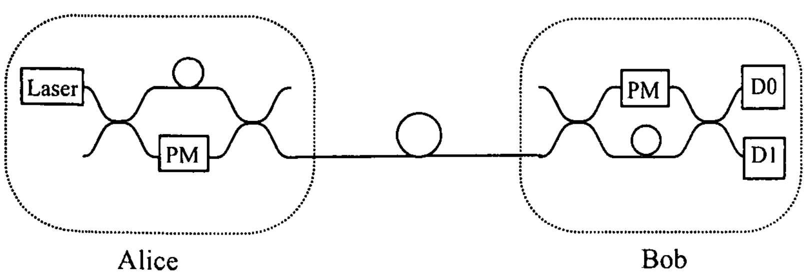


Fig. 2.7. Phase setup with a collapsed Mach–Zehnder interferometer: Instead of having the two pulses propagating through different paths, they now propagate through the same optical fibre, but with a time-delay. This increases the stability of the interferometer, but adds 3 dB of losses in Bob's setup.

the pulses actually follow the same path for most of the interferometer. The drawback is that we lose half of the signal in the two SS and LL paths.

The scheme proposed by C. Bennett [45], used only two phases for Alice. We refer the reader to the original article for a detailed explanation. The main advantage of this type of systems is that, in principle, it does not require polarisation control. In practice, however, due to some polarisation dependence in the components, it seems preferable to control the polarisation. Moreover, these schemes still need careful path length adjustment and control between the two sides of the interferometer.

2.4 Quantum Key Distribution with Entangled States

2.4.1 Transmission of the Raw Key

The key distribution is performed via a quantum channel which consists of a source that emits pairs of photons in the singlet state of polarisations:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|\updownarrow\rangle|\leftrightarrow\rangle - |\leftrightarrow\rangle|\updownarrow\rangle\right) \tag{2.10}$$

The photons fly apart along the z-axis towards the two legitimate users of the channel, Alice and Bob, who, after the photons have separated, perform measurements and register the outcome of the measurements in one of three bases, obtained by rotating the $\oplus$ basis around the z-axis by angles $\phi_1^a = 0, \phi_2^a = \frac{1}{4}\pi, \phi_3^a = \frac{1}{8}\pi$ for Alice and by angles $\phi_1^b = 0, \phi_2^b = -\frac{1}{8}\pi, \phi_3^b = \frac{1}{8}\pi$ for Bob.

Superscripts "a" and "b" refer to Alice's and Bob's analysers respectively. The users choose their bases randomly and independently for each pair of the incoming particles. Each measurement yield two possible results, +1 (the photon is measured in the first polarisation state of the chosen basis) and -1 (it is measured in the other polarisation state of the chosen basis), and can potentially reveal one bit of information.

The quantity

$$E(\phi_i^a, \phi_j^b) = P_{++}(\phi_i^a, \phi_j^b) + P_{--}(\phi_i^a, \phi_j^b) - P_{+-}(\phi_i^a, \phi_j^b) - P_{-+}(\phi_i^a, \phi_j^b) \tag{2.11}$$

is the correlation coefficient of the measurements performed by Alice in the basis rotated by ϕ_i^a and by Bob in the basis rotated by ϕ_j^b. Here $P_{\pm\pm}(\phi_i^a, \phi_j^b)$ denotes the probability that the result ±1 has been obtained in the basis defined by ϕ_i^a and ±1 in the basis defined by ϕ_j^b. According to the quantum rules

$$E(\phi_i^a, \phi_j^b) = -\cos\left[2(\phi_i^a - \phi_j^b)\right]. \tag{2.12}$$